

Форма № ДН-7.02.1

Державний вищий навчальний заклад
«Донецький національний технічний університет»
Кафедра Прикладної математики та інформатики



«ЗАТВЕРДЖУЮ»

Перший проректор

Леонід Бачурін

2020 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Системи технічного захисту інформації

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність (ості) 125 Кібербезпека

(шифр і назва спеціальності (тей))

Освітня програма Кібербезпека

(назва освітньої програми)

Мова навчання: українська

Покровськ – 2020

Робоча програма навчальної дисципліни «Системи технічного захисту інформації»

(повна назва дисципліни)

для здобувачів вищої освіти за спеціальністю 125 Кібербезпека

«19» вересня 2020 року. – 7 с.

Розробники: (вказати авторів, їхні наукові ступені, вчені звання та посади).

ст. викладач кафедри прикладної математики та інформатики

Скрипник Т.В.

Робоча програма затверджена на засіданні кафедри прикладної математики
і інформатики

(назва кафедри)

Протокол № 11 від «1» травня 2020 р.

Завідувач кафедрою прикладної математики та інформатики

(підпис)

(Дмитрієва О.А.)

(прізвище та ініціали)

«1» травня 2020 р.

Схвалено науково-методичною комісією з галузі знань 12 Інформаційні технології

(шифр, назва)

Протокол № 6 від «7» травня 2020 р.

«7» травня 2020 р. Голова

(підпис)

(Башков Є.О.)

(прізвище та ініціали)

1. Загальна інформація

Форма навчання	Денна	Заочна
Статус	вибіркова	
Обсяг в кредитах ЄКТС	6	—
Обсяг в годинах за навчальним планом, разом: в тому числі:	180	—
лекції:	32	—
практичні заняття:	32	—
лабораторні заняття:		—
семінари:		—
самостійна робота:	116	—
Форма підсумкового контролю	Екзамен	
Дисципліну викладають	Викладач 1 (Скрипник Т.В., https://donntu.edu.ua/knt/pmi , tetiana.skrypnyk@donntu.edu.ua) Викладач 2 (Черняк Т.О. https://donntu.edu.ua/knt/pmi , tetiana.cherniak@donntu.edu.ua)	

Передумови для вивчення дисципліни: Основи інформаційної безпеки, Безпека та захист операційних систем, Математичні методи криптографії, Безпека програм та даних, Вища математика.

2. Мета вивчення навчальної дисципліни

Метою викладання дисципліни є формування у студентів здатностей зі стиснення та шифрування даних, кодування та стиснення інформації, що передається, аналіз та тестування алгоритмів шифрування та розшифрування, логічного та аналітичного мислення в прийнятті рішень щодо безпечної передачі та збереження даних.

Завдання дисципліни: навчити студентів застосовувати та аналізувати різні фундаментальні та вдосконалені алгоритми для стиснення та шифрування даних, опанувати основні методи аналізу алгоритмів, набуті вміння будувати та здійснювати раціональний вибір алгоритму для конкретної складної спеціалізованої задачі з відомих класів алгоритмів на основі обраних критеріїв.

Компетентності:

- Здатність адаптуватися в умовах частой зміни технологій професійної діяльності, прогнозувати кінцевий результат.
- Здатність діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та/або кібербезпеки.
- Здатність вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- Здатність ідентифікувати, класифікувати та формулювати вимоги до спеціалізованого програмного забезпечення.
- Здатність вирішувати задачі аналізу програмного коду на наявність можливих загроз.

- Здатність накопичувати, обробляти та систематизувати професійні знання щодо захисту і безпечного супроводження програмного забезпечення та визнання важливості навчання протягом всього життя.
- Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.
- Здатність вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

Програмні результати навчання:

- Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.
- Уміння вибирати та використовувати відповідну до задачі методологію створення програмного забезпечення.
- Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
- Знати і застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

3. Очікувані результати навчання

В результаті вивчення даного курсу студент повинен

знати:

- основні алгоритми стиснення різних типів даних;
- основні поняття криптографічного захисту інформації;
- класифікацію криптографічних алгоритмів;
- основні види алгоритмів стиснення і шифрування різних структур даних;
- принципи проектування та тестування криптографічних алгоритмів;
- найбільш розповсюджені методи криптоаналізу.

вміти:

- розробляти та застосовувати криптографічні алгоритми;
- обґрунтовувати застосування механізмів захисту та оцінки рівня захищеності інформаційної системи (технології);
- застосовувати різні методи стиснення при передачі різних структур даних;
- визначати моделі, принципи і правила побудови систем криптографічного захисту від несанкціонованого доступу об'єктів і інформаційно-комунікаційних систем;

4. Засоби діагностики результатів навчання

Перевірка й оцінювання знань студентів здійснюється методами усного, письмового, практичного контролю та самоконтролю.

При **поточному** контролі оцінці підлягають:

– результати виконання і захисту **практичних робіт**;

Поточний контроль має на меті перевірку рівня підготовленості студента до виконання конкретної роботи. Поточний контроль проводиться на лабораторних заняттях.

Поточний контроль здійснюється за двома напрямками:

- контроль за систематичністю та активністю роботи на заняттях під час виконання лабораторних робіт;

Семестровий контроль проводиться за формою: **семестровий іспит**, в обсязі навчального матеріалу, визначеного навчальною програмою, і в терміни, встановлені навчальним планом.

Форма проведення іспиту – письмова.

Під час семестрового контролю враховуються результати здачі усіх видів навчальної роботи згідно із структурою залікових кредитів.

5. Критерії оцінювання результатів навчання

Оцінювання знань студента здійснюється за 100-бальною шкалою.

Пр.1	Пр.2	Пр.3	Пр.4	Пр.5	Пр.6	Поточний контроль	Іспит	Максимальний бал
5	5	10	10	5	5	40	60	100

В цьому розділі наводиться також схема оцінювання з урахуванням вимог Положення про організацію освітнього процесу. Результати підсумкового контролю оцінюються за 100-бальною шкалою та чотирибальною («відмінно», «добре», «задовільно», «незадовільно»). Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену, курсового проекту(роботи), практики, диференційованого заліку, кваліфікаційного екзамену, випускної кваліфікаційної (дипломної) роботи (проекту)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

ТЕМА 1. Загроза інформації та можливості її прихованої передачі.

ТЕМА 2. Основні поняття стеганографії.

ТЕМА 3. Характеристика сучасних кібератак на інформаційно-телекомунікаційні системи та інформаційні ресурси.

ТЕМА 4. Програмно-апаратні засоби захисту інформаційно-телекомунікаційних систем.

ТЕМА 5. Основні поняття криптографії. Популярні алгоритми шифрування даних.

ТЕМА 6. Засоби паролльної ідентифікації та адміністрування.

ТЕМА 7. Використання електронного підпису.

ТЕМА 8. Алгоритми симетричного шифрування даних.

ТЕМА 9. Асиметричні криптографічні системи шифрування.

ТЕМА 10. Формування загальних вимог до КСЗІ в ІКС.

ТЕМА 11. Система управління інформаційною безпекою підприємства

ТЕМА 12. Нормативно-правове забезпечення в сфері інформаційної безпеки.

6.2. Теми практичних (семінарських) занять

№ з/п	Назва теми		Кількість годин	
			Д.ф.н.	З.ф.н.
1	Тема 1-2	Практична робота 1. Дослідження вільного ПЗ для стеганографічних методів передачі даних	4	–
2	Тема 2	Практична робота 2. Дослідження вільного ПЗ для криптографічних перетворень даних	4	–
3	Тема 1-2	Практична робота 3. Дослідження та аналіз найуживанішого ПЗ для криптоаналізу	6	–
4	Тема 3-5	Практична робота 4. Дослідження апаратних та програмних методів захисту інформації	10	–
5	Тема 6-9	Практична робота 5. Дослідження асиметричних методів шифрування. Алгоритм RSA.	4	–
6	Тема 6-9	Практична робота 6. Дослідження алгоритму несиметричного цифрового підпису Ель-Гамала	4	–
Усього за семестр			32	

6.3. Теми лабораторних занять

№ з/п	Назва теми		Кількість годин	
			Д.ф.н.	З.ф.н.
1	Проведення лабораторних занять програмою не передбачено			
...	Усього годин			

6.4. Самостійна робота

№ з/п	Назва теми		Кількість годин	
			Д.ф.н.	З.ф.н.
1.	СРС теми 3. Класифікація сучасних кібератак		10	
2.	СРС теми 4. Шифри підстановки. Шифри перестановки		10	
3.	СРС теми 4. Блокові шифри як групові математичні перестановки		10	
4.	СРС теми 5. Класифікація поточкових шифрів. Генератор псевдовипадкових чисел на основі алгоритму <i>BBS</i>		8	
5.	СРС теми 6. Подвійний <i>DES</i> . Потрійний <i>DES</i> .		8	
6.	СРС теми 7. Режим виконання "Електронна кодова книга", "Зчеплення блоків зашифрованих даних", "Зворотний зв'язок"		8	
7.	СРС теми 7. Генерація раундових ключів. Безпека шифру <i>IDEA</i> .		8	
8.	СРС теми 8. Шифрування даних у режимі гамування. Шифрування даних у режимі утворення імітовставки.		8	
9.	СРС теми 8. Мультиплікативні та адитивні операції. Раундові перетворення алгоритму		8	
10.	СРС теми 9. Криптографічні системи Діффі-Хеллмана, Ель-Гамала, Рабіна.		8	
11.	СРС теми 10. Формування загальних вимог до КСЗІ в ІКС		10	

12.	СРС теми 11 Система управління інформаційною безпекою підприємства.	10	
13.	СРС теми 12. Нормативно-правове забезпечення в сфері інформаційної безпеки	10	
	Усього годин	116	

6.5. Індивідуальні та/або групові завдання

У рамках курсу передбачено виконання розрахункової роботи на тему «Дослідження та аналіз стеганографічних та криптографічних методів передачі даних».

7. Література

7.1. Основна

1. Брюс Шнайер, Нильс Фергюсон. - Практическая криптография. — М. «Вильямс» - 2016, 420 с.
2. Е. Яковенко, И. Журавель и др. - Інформаційна безпека. – «Львівська політехніка» - 2019, 580 с.
3. Кер Сенкер - .Cybercrime and the Darknet, - «Arcturus» – 2017, 192 с.
4. М. Адаменко, - Основы классической криптологии. Секреты шифров и кодов – ДМК Пресс – 2012, 256 с.
5. Л. Бабенко, А. Басан, И. Журкин. - Защита данных геоинформационных систем,- «Гелиос АРВ» - 2010, 336 с.
6. Юрий Диогенес, Эрдаль Озкайя. - Кибербезопасность. Стратегии атак и обороны, - ДМК Пресс – 2016, 326 с.

7.2. Допоміжна

1. Математичні методи захисту інформації. Курс лекцій. Ч І. / Укладачі Завадська Л.О., Савчук М.М. – К.: НТУУ «КПІ», 2008. – 128 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. - М.: Издательство ТРИУМФ, 2003. - 816 с.

7.3. Методична

1. Методичні рекомендації до проведення практичних занять з дисципліни (в розробці).
2. Методичні рекомендації до самостійного вивчення дисципліни (в розробці).